NTP の設定

この章では、Cisco MDS 9000 シリーズ スイッチ デバイスでネットワーク タイム プロトコル（NTP）を構成する方法について説明します。

NTP の概要

ここでは、NTP の情報について説明します：

NTP

規模の大きい企業ネットワークでは、複数の装置間で記録される相互作用イベントのアソシエーションを試みる場合、すべてのネットワーク装置で1つの時間基準を持つことは、管理レポーティングおよびイベントロギング機能において重要です。重要なネットワークを保有する多くの企業のお客様は、独自のストラタム 1 NTP ソースを保持しています。

クライアントとサーバー間で複数のフレームが交換されたときに時刻の同期化が行われます。クライアント モードにあるスイッチは、1 つまたは複数の NTP サーバのアドレスを認識します。NTP サーバはタイム ソースとして動作し、クライアントの同期要求を受け取ります。

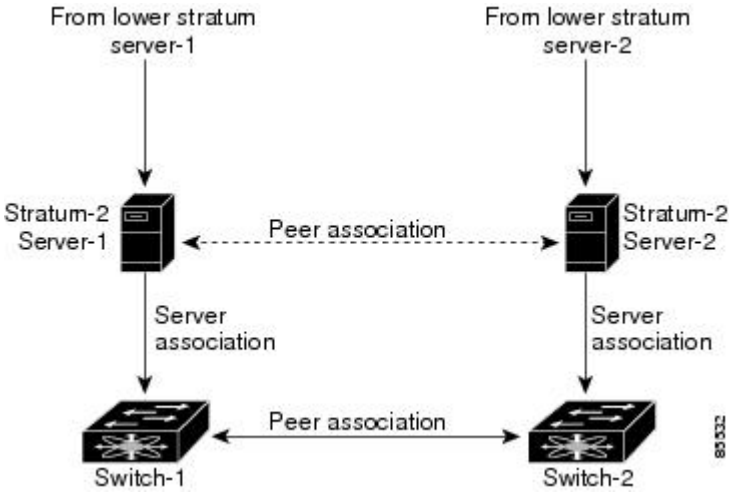
ピアとして IP アドレスを設定することによって、Cisco NX-OS device は必要に応じて時刻を入手し、提供できます。ピアでは、独自に時刻を提供することができ、サーバが設定されている場合も対応できます。これらの両方のインスタンスが別のタイム サーバーに指定される場合、NTP サービスがより信頼性の高いものになります。現用系サーバー リンクが失われた場合でも、ピアの存在によって正確な時間を保つことができます。

アクティブ サーバに障害が発生する場合、設定されたピアが NTP 時刻の提供に役立ちます。現用系サーバーに機能不全が発生した場合のバックアップ サポートを確保するには、直接的な NTP サーバー アソシエーションを指定して、ピアを設定します。

ピアだけを構成すると、最も正確なピアが NTP サーバーの役割を引き受け、他のピアがピアとして動作します。両方のデバイスが正確なタイム送信元を持つ場合、または正確なNTP送信元を指定する場合、適切な時間に終了します。

図 *1: NTP* のピアおよびサーバー アソシエーション

ネットワーク内に適切に設定されているスイッチはサーバのダウンタイムにも影響されません。この図に、2 つの NTP ストラタム 2 サーバーおよび 2 つのスイッチを含むネットワークを示します。



この設定では、スイッチは次のように設定されています。

- Stratum-2 Server-1
  - IPv4 アドレス -10.10.10.10
- Stratum-2 Server-2
  - IPv4 アドレス -10.10.10.9
- Switch-1 IPv4 アドレス -10.10.10.1
- Switch-1 NTP 構成
  - NTP サーバ 10.10.10.10
  - NTP ピア 10.10.10.2
- Switch-2 IPv4 アドレス -10.10.10.2
- Switch-2 NTP 構成
  - NTP サーバ 10.10.10.9

• NTP ピア 10.10.10.1

NTP の前提条件

NTP の前提条件 は、次のとおりです。

• スイッチには、他の NTP 対応デバイスへの IP 接続が必要です。

NTP の注意事項と制約事項

NTP に関する設定時の注意事項および制約事項は、次のとおりです。

• スイッチのクロックの信頼性が高い（高品質のローカルクロックがあるか、スイッチ自体が信頼できる NTP サーバーのクライアントである）ことが確実な場合にのみ、別のデバイスとのピア アソシエーションを許可する必要があります。

• 単独で設定したピアは、サーバーの役割を担いますが、バックアップとして使用する必要があります。サーバが 2 台ある場合、いくつかのデバイスが一方のサーバに接続し、残りのデバイスが他方のサーバに接続するように設定できます。その後、2 台のサーバ間にピア アソシエーションを設定すると、信頼性の高い NTP 構成になります。

• サーバが 1 台だけの場合は、すべてのデバイスをそのサーバのクライアントとして設定する必要があります。

• 設定できる NTP エンティティ（サーバおよびピア）は、最大 64 です。

NTP の設定

ここでは、NTP の設定方法について説明します。

NTP をイネーブル化

スイッチで NTP を有効にするには：

Note NTP はデフォルトでイネーブルです。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP イネーブル化：

switch(config)# **feature ntp**

NTP のディセーブル化

スイッチで NTP を無効にするには：

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP を無効にします：

switch(config)# **no feature ntp**

認証キーの設定

ntp trusted-key コマンドにより、デバイスが、信頼されていない時刻源と誤って同期する、ということが防止されます。サーバー デバイスのタイム ゾーンをクライアント デバイスのタイム ゾーンと同期させるには、サーバー デバイスでのみ NTP 認証機能を有効にすることができます。クライアント デバイスのタイム ゾーンをサーバー デバイスのタイム ゾーンと同期するには、両方のデバイスで NTP 認証機能を有効にする必要があり、クライアント デバイスで指定されたキーは、サーバー デバイスで指定されたキーの 1 つである必要があります。サーバー デバイスとクライアント デバイスで指定されたキーが異なる場合、サーバー デバイスのタイム ゾーンのみがクライアント デバイスのタイム ゾーンと同期できます。

NTP アソシエーションの認証に使用するキーを設定するには、次の手順を実行します。

始める前に

この手順で指定する予定の認証キーによって、NTP サーバが設定されていることを確認します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 認証キーを定義します：

switch(config)# **ntp authentication-key** *id* **md5** *key* [**0** | **7**]

key 識別子 の範囲は 1 ～ 65535 です。 *key* は、最大 8 文字の英数字を入力できます。

ステップ 3 1 つ以上のキーを指定します。デバイスが時刻ソースと同期するために、時刻送信元はこのキーを NTP パケット内に提供する必要があります。

switch(config)# **ntp trusted-key** *id*

key 識別子 の範囲は 1 ～ 65535 です。

次のタスク

一時、対称、ブロードキャスト、またはマルチキャスト NTP アソシエーションの認証の有効化 （5 ページ）.

一時、対称、ブロードキャスト、またはマルチキャスト NTP アソシエーションの認証の有効化

信頼できないソースがデバイスに更新を注入するのを防ぐために、（サーバーまたはピアの更新とは対照的に）一時、対称、ブロードキャスト、またはマルチキャストの更新を認証する必要があります。

これらのタイプの NTP アソシエーションの認証を有効にするには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 リモート ネットワーク ホストとの新しい一時、対称、ブロードキャスト、またはマルチキャスト アソシエーションからのパケットの NTP 認証を有効にします（これは、 **ntp server**コマンドまたは **ntp peer**コマンドを使用して作成されたピア アソシエーションを認証しません）。

switch# **ntp authenticate**

一時、対称、ブロードキャスト、またはマルチキャスト NTP アソシエーションの認証の無効化

これらのタイプの NTP アソシエーションの認証を無効にするには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 リモート ネットワーク ホストとの新しい一時、対称、ブロードキャスト、またはマルチキャスト アソシエーションからのパケットの NTP 認証を無効にします (これは、 **ntp server**コマンドまたは **ntp peer**コマンドを使用して作成されたピア アソシエーションを認証しません)。

switch(config)# **no ntp authenticate**

NTP 認証はデフォルトでディセーブルになっています。

NTP サーバーとピアの有効化

NTP サーバーは、NTP 更新の信頼できる送信元です。ローカル デバイスはサーバーの時刻に従いますが、サーバーはローカル デバイスの時刻から更新されません。NTP ピアは更新を送信し、受信したピア更新に調整して、すべてのピアが同時に収束するようにします。デバイスは、複数のサーバーまたはピアに関連付けられている場合があります。

NTP は、キーによる認証を導入します。NTP キーを使用して、信頼できるデバイスのみに交換をフィルタ処理します。これにより、誤って構成された、または悪意のある送信元からの NTP 更新を信頼することを回避できます。

NTP サーバーとピアをイネーブル化するには、次のステップを実行します：

Before you begin

使用しているNTPサーバーと、そのピアのIPアドレスまたはドメイン ネーム システム（DNS）名がわかっていることを確認します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 1 つのサーバーと 1 つのサーバー アソシエーションを形成します：

switch(config)# **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *id*] [**prefer**] [**maxpoll** *interval*] [**minpoll** *interval*]

複数のサーバー アソシエーションを指定できます。

key キーワードを使用して、指定されたキーを使用して指定されたサーバーでの認証を有効にします。*id* 引数の範囲は 1 ～ 65535 です。

このサーバーをデバイスの優先 NTP サーバーにするには、 **prefer** キーワードを使用します。

サーバーをポーリングする最大および最小の間隔を構成するには、 **maxpoll** と **minpoll** キーワードを使用します。インターバルの範囲は、4 から 16 秒です。maxpoll のデフォルト値は、6 で、minpoll のデフォルト値は、4 です。

Note NTP サーバとの通信で使用するキーを設定する場合は、そのキーが、デバイス上の信頼できるキーとして存在していることを確認してください。

ステップ 3 ピアとのアソシエーションを形成します：

switch(config)# **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *id*] [**prefer**] [**maxpoll** *interval*] [**minpoll** *interval*]

複数のピア アソシエーションを指定できます。

key キーワードを使用して、指定されたキーを使用して指定されたサーバーでの認証を有効にします。*id* 引数の範囲は 1 ～ 65535 です。

デバイスに対して対象の NTP ピアを優先にするには、**prefer** キーワードを使用します。

ピアをポーリングする最大および最小の間隔を設定するには、 **maxpoll** と **minpoll** キーワードを使用します。インターバルの範囲は、4 から 17 秒です。maxpoll のデフォルト値は、6 で、minpoll のデフォルト値は、4 です。

Note NTP ピアとの通信で使用するキーを構成する場合は、そのキーが、デバイス上の信頼できるキーとして存在していることを確認してください。

NTP サーバーとピアのディセーブル化

NTP サーバーとピアをディセーブル化するには、次のステップを実行します：

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP サーバーをディセーブル化します：

switch(config)# **no ntp server** {*ip-address* | *ipv6-address* | *dns-name*}

ステップ 3 NTP ピアをディセーブル化します：

switch(config)# **no ntp peer** {*ip-address* | *ipv6-address* | *dns-name*}

NTP モードをイネーブル化

NTP 制御モードおよびプライベート モード パケットの処理を有効にするには、次の手順を実行します：

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 コントロール モードおよびプライベート モード パケットの処理を有効にします。

switch(config)# **ntp allow** {**private** | **control** [**rate-limit** *seconds*]}

デフォルトの持続時間は 3 秒です。これは、制御モード パケットが 3 秒ごとに処理または応答されることを意味します。値の範囲は 1 ～ 65535 です。

NTP モード のディセーブル化

NTP 制御モードおよびプライベート モード パケットの処理をディセーブル化にするには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 コントロール モードとプライベート モードのパケットの処理を無効にします。

switch(config)# **no ntp allow** {**private** | **control** [**rate-limit** *seconds*]}

送信元インターフェイスでの NTP のイネーブル化

スイッチから送信される NTP パケットのデフォルトの送信元アドレスを上書きするには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 スイッチから送信される NTP パケットのデフォルトの送信元アドレスを上書きします。

switch(config)# **ntp source-interface** {**ethernet** *slot/port.sub-interface* | **mgmt** *number* | **port-channel** *number*}

指定できる **ntp source-interface** コマンドは 1 つだけです。すべてのインターフェイスを介して送信されるすべての NTP パケットは、このコマンドで指定されたアドレスを送信元アドレスとして使用します。

送信元インターフェイスでの NTP のディセーブル化

NTP パケットのデフォルトの送信元アドレスを復元するには、次の手順を実行します：

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP パケットのデフォルトの送信元アドレスを復元します：

switch(config)# **no ntp source-interface** {**ethernet** *slot/port.sub-interface* | **mgmt** *number* | **port-channel** *number*}

NTP ロギングをイネーブル化します。

NTP メッセージの syslog へのロギングを有効にするには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP ロギングをイネーブル化します：

switch(config)# **ntp logging**

NTP ロギングを無効化

syslog への NTP メッセージのロギングを無効にするには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP ロギングを無効にします：

switch(config)# **no ntp logging**

NTP Syslog ロギング レベルの構成

NTP Syslog メッセージの重大度しきい値を設定するには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP Syslog メッセージの重大度しきい値を構成します：

switch(config)# **logging level ntp** {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7**}

次のキーワードは、重大度レベルを指定します：

- **0** —ログに緊急事態メッセージを指定します。
- **1** — アラート メッセージをログに記録することを指定します。
- **2** — ログに重大メッセージを指定します。
- **3** — ログにエラーメッセージを指定します。

- **4** — 警告メッセージをログに記録することを指定します。
- **5** — 通知メッセージをログに記録することを指定します。
- **6** — 情報メッセージをログすることを指定します。
- **7** — デバックメッセージをログに記録することを指定します。

デフォルトの NTP Syslog 重大度ログ レベルの設定

デフォルトの NTP syslog 重大度ロギング レベルに戻すには、次の手順を実行します：

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 デフォルトの NTP syslog 重大度ロギング レベルに戻ります：

switch(config)# **no logging level ntp** {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7**}

NTP 統計のクリアと表示

NTP は、必要に応じて表示および消去できる統計を生成します。

NTP 統計を表示およびクリアするには、次の手順を実行します：

ステップ 1 NTP 統計情報を表示します：

switch# **show ntp statistics** {**peers** | **io** | **local** | **memory**}

次の NTP 統計を表示できます：

- **peer**—ピアごとの NTP 統計。
- **io**— NTP パケット処理の統計。
- **local**— NTP パケット タイプの統計。
- **memory**— NTP によるメモリ使用量の統計。

ステップ 2 NTP の統計情報をクリアします：

switch# **clear ntp statistics** {**peer** | **io** | **local** | **memory**}

NTP の再同期

スイッチの NTP クライアントがサーバーまたはピアとの同期を失った場合、NTP クライアントを再起動する必要がある場合があります。これにより、ローカル スイッチで構成されているすべての NTP サーバーとピアとの同期プロセスが再開されます。NTP サーバーとクライアントのステータスを確認するには、NTP のトラブルシューティングセクションを参照してください。

スイッチ上の NTP クライアントを再起動するには、次の手順を実行します：

同期を再試行：

switch# **ntp sync-retry**

CFS を使用した NTP 構成の配布

CFS を使用して、ファブリック内の他のスイッチにローカル NTP 構成を配布できます。

（注） CFS を介して配布されるのは、NTP サーバーとピアの構成だけです。

NTP 構成流通のイネーブル化

NTP 設定の CFS 配信をイネーブル化するには、次の手順を実行します。

始める前に

- CFS がイネーブルになっていることを確認します。詳細については、Cisco MDS 9000 Series System Management Configuration Guide内の「CFS 配布ステータスを検証」セクションを参照してください。
- NTP がイネーブル化されていることを確認します。詳細については、「NTP の確認 （13 ページ）」を参照してください。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP 設定の配信をファブリック内のすべてのスイッチでイネーブル化します：

switch(config)# **ntp distribute**

このコマンドは、ファブリックのロックを取得して、その後の設定変更をすべて保留データベースに格納します。

NTP 構成配布の無効化

NTP 設定の CFS 配信を無効にするには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 NTP 構成の配布を無効にします。

switch(config)# **no ntp distribute**

NTP 設定変更のコミット

NTP 構成の変更をコミットすると、Cisco NX-OS ソフトウェアは、保留中の変更をローカル Cisco MDS スイッチの実行構成と、NTP 構成配信を受信できるファブリック内のすべての Cisco MDS スイッチに適用します。

保留中の NTP 構成をファブリック内の NTP CFS 対応ピアに適用するには、次の手順を実行します。

始める前に

別の Cisco MDS スイッチ内のファブリックの NTP 構成流通をイネーブル化します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 保留中の NTP 構成を、ファブリック内の NTP CFS 対応ピアに配布します。

switch(config)# **ntp commit**

NTP 設定変更の廃棄

NTP配布モードでは、構成の変更は、ユーザーがコミットするまでバッファリングされます。**abort** コマンドでコミットされる前に、変更を破棄できます。

スイッチで既存の NTP CFS 配信セッションを終了してロックを解除するには、次の手順を実行します。

ステップ 1 次の設定モードを入力します。

switch# **configure terminal**

ステップ 2 スイッチ上の既存の NTP CFS 配信セッションを終了してロックを解除します：

switch(config)# **ntp abort**

失われた NTP 構成セッションの強制終了

ユーザーが配布モードで NTP 構成の変更を開始すると、セッションが作成され、CFS がファブリック全体のセッション ロックを作成します。セッション ロックは、他のユーザーが同時にセッションを作成し、NTP 構成を変更することを防止するためのものです。ユーザーが変更をコミットまたはキャンセルしない場合、ロックが解除されるまで、以降の NTP 構成セッションは阻止されます。この場合、セッション ロックは別のユーザーによってリリースされる可能性があり、このアクションにより、セッション内の保留中のすべての NTP 構成変更が破棄され、ロックが解放されます。セッション ロックのリリースは、ファブリック内のどのスイッチからでも実行できます。管理者がこのタスクを実行すると、保留中の構成変更は廃棄され、ファブリック ロックがリリースされます。

管理者権限を使用し、ロックされた NTP セッションをリリースする手順は、次の手順を実行します：

ロックされた NTP セッションをリリースします：

switch# **clear ntp session**

NTP の確認

次のコマンドを使用して、NTP を確認します：

次に、NTP がイネーブル化されていることを確認する例を表示します：

```
switch(config)# show running-config all | include "feature ntp"
feature ntp
```

次に、現在の NTP 構成を表示する例を表示します：

```
switch# show running-config ntp

!Command: show running-config ntp
!Time: Fri Jan 1 1:23:45 2018
```

```
version 8.2(1)
logging level ntp 6
ntp peer 192.168.12.34
ntp server 192.168.86.42
ntp authentication-key 1 md5 fewhg12345 7
ntp logging
```

この例は、現在のセッションのコミットされていない（保留中の）NTP構成を示しています：

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# ntp peer 192.168.12.34
switch(config)# show ntp pending peers

ntp peer 192.168.12.34

switch(config)# ntp commit
switch(config)# show ntp pending peers
```

保留 CFS データベースと現行の NTP 構成の差異をこの例は、表示します：

```
switch# show ntp pending-diff
```

次の例は、次の **time-stamp** コマンドを使用してタイム スタンプ チェックが有効になっているかどうかを示しています。

```
switch# show ntp timestamp status
Linecard 3 does not support Timestamp check.
```

NTP のトラブルシューティング

NTP のトラブルシューティングには、次の情報を使用します。

この例は、NTP CFS ステータスを示しています。

```
switch# show ntp status
Distribution : Disabled
Last operational state: No session
```

次の例は、NTP 構成の変更がどのスイッチに配布されるかを確認する方法を示しています：

```
switch1# show cfs peers name ntp

Scope : Physical-fc-ip
--------------------------------------------------------------------------
Switch                  WWN IP Address
--------------------------------------------------------------------------
20:00:8c:60:4f:0d:2b:b0 192.168.12.34 [Local]
                        [switch1]
20:00:8c:60:4f:0d:32:d0 192.168.56.78 [Merged]
                        [switch2.mydomain.com]
```

```
Total number of entries = 2
```

この例は、NTP セッション情報を表示します：

```
switch# show ntp session status
Last Action Time Stamp     : None
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : none
```

この例は、すべての NTP ピアを表示します：

```
switch# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  10.105.194.169                Server (configured)
```

この例は、**show ntp pending peers** コマンドと **show ntp pending-diff** コマンドの違いを表示します。出力は、NTP サーバーまたはピアを追加した場合と同様です。

```
switch1# configure terminal
switch1(config)# ntp authenticate
switch1(config)# ntp authentication-key 1 md5 aNiceKey
switch1(config)# ntp server 192.168.12.34 key 1
switch1(config)# ntp authentication-key 2 md5 goodTime
switch1(config)# ntp peer 192.168.56.78 key 2
switch1(config)# show ntp pending peers

ntp server 192.168.12.34


ntp peer 192.168.56.78

switch1(config)# show ntp pending-diff
+ntp peer 192.168.56.78
+ntp server 192.168.12.34
switch1(config)# ntp commit
switch1(config)# show ntp pending peers
switch1(config)# show ntp pending-diff
```

注意 サーバーおよびピア コマンドのみが NTP ピア スイッチに配布されます。認証の有効化や認証キーの設定などの他のパラメータは、各スイッチで構成する必要があります。

スイッチ 1 の例を続けると、サーバーまたはピアを削除すると出力が異なります。

```
switch1(config)# no ntp peer 192.168.56.78
switch1(config)# show ntp pending peers

ntp server 192.168.12.34

switch1(config)# show ntp pending-diff
-ntp peer 192.168.56.78
```

```
switch1(config)# ntp commit
switch1(config)# show ntp pending peers
switch1(config)# show ntp pending-diff
switch1(config)# end
```

この例は、ピアのステータスを示しています。各ピアに関する情報が、1 回線に 1 つのピアとして表に表示されます。各行の最初の文字はステータス フラグです。表の上の凡例は、このフラグの意味を表示しています。同期してローカル時刻の更新に使用される NTP サーバーとピアには、等号（=）フラグがあります。更新されるローカル スイッチの時間に対して、このフラグを持つデバイスが少なくとも 1 つ必要です。パッシブ ピアは、現在同期されていないピアです。これは、ローカル スイッチがこれらのピアからの時刻更新を使用しないことを意味します。リモート 列には、ピアの送信元 IP アドレスが表示されます。ピアの送信元 クロックまたはストラタムの正確度は、*st* 列に表示されます。stratum の値が高いほど、ピアのクロック 送信元の精度が低くなり、16 が最も低い正確度になります。秒数の投票間隔は、投票 列で表示されています。リーチ 列の到達可能性フィールドは、そのピアとの最後の 8 つのトランザクションの循環ビットマップであり、「1」は成功を示し、「0」は失敗を示し、最下位ビットの最新のトランザクションを示します。このピアは、最後の 6 つのポーリング メッセージを失っていません。ローカル スイッチとピア間の往復時間（秒単位）は、遅延 列に表示されます。

```
switch# show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode
    remote           local    st   poll   reach delay
-------------------------------------------------------------------
*10.105.194.169     0.0.0.0    4     16      77   0.00099
```

この例は、単一のサーバーまたはピアの詳細な NTP 情報を示しています。

最後に受信したパラメータは、そのサーバーまたはピアからフレームを受信するたびにゼロに戻ります。したがって、ピアが到達不能であるか、ローカル スイッチの NTP クライアントに送信していない場合、このパラメータは着実に増加します。

```
switch# show ntp statistics  peer ipaddr 10.105.194.169
remote host:          10.105.194.169
local interface:      Unresolved
time last received:   9s
time until next send: 54s
reachability change:  54705s
packets sent:         3251
packets received:     3247
bad authentication:   0
bogus origin:         0
duplicate:            0
bad dispersion:       0
bad reference time:   0
candidate order:      6
```

次の例は、スイッチのローカル NTP クライアントによって維持されるカウンタを示しています。

```
switch# show ntp statistics local
```

```
system uptime:          24286
time since reset:       24286
old version packets:    13
new version packets:    0
unknown version number: 0
bad packet format:      0
packets processed:      13
bad authentication:     0
```

例: NTP を構成

次の例は、NTP プロトコルをイネーブル化にする方法を示しています。

```
switch# configure terminal
switch(config)# feature ntp
```

次の例は、NTP プロトコルをディセーブル化にする方法を示しています。

```
switch# configure terminal
switch(config)# no feature ntp
```

次の例は、NTP サーバーを構成する例を表示します。

```
switch# configure terminal
switch(config)# ntp server 192.0.2.10
```

次の例は、NTP ピアを設定する方法を表示しています：

```
switch# configure terminal
switch(config)# ntp peer 2001:0db8::4101
```

次の例は、NTP 認証を設定する方法を表示しています：

```
switch# configure terminal
switch(config)# ntp authentication-key 42 md5 key1_12
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
```

次の例は、プライベート モード パケットの処理をイネーブルにする方法を示しています：

```
switch# configure terminal
switch(config)# ntp allow private
```

次の例は、レート制限が10秒の制御モードパケットの処理を有効にする方法を示しています：

```
switch# configure terminal
switch(config)# ntp allow control rate-limit 10
```

次の例は、NTP 送信元 インターフェイスを構成する方法を表示しています：

```
switch# configure terminal
switch(config)# ntp source-interface ethernet 2/2
```

この例では、syslog への NTP メッセージのロギングを有効にし、syslog ロギングのしきい値を「情報」に変更します。

```
switch# configure terminal
switch(config)# ntp logging
switch(config)# logging logfile messages 6
switch(config)# end
switch# show logging | include "logfile:" next 1
Logging logfile: enabled
Name - messages: Severity - information Size - 4194304
switch# show logging logfile | include %NTP
2017 Jan 1 1:02:03 switch %NTP-6-NTP_SYSLOG_LOGGING: : Peer 192.168.12.34 is reachable
2017 Jan 1 2:34:56 switch %NTP-6-NTP_SYSLOG_LOGGING: : System clock has been updated,
offset= sec
```

次に、NTP のロギングをディセーブルにする例を表示します。

```
switch# configure terminal
switch(config)# no ntp logging
```

NTP のデフォルト設定

次の表に、NTP パラメータのデフォルト設定を示します。

表 *1:* デフォルトの *NTP* 設定

NTP	無効
NTP モード	無効
NTP 送信元インターフェイス	mgmt0
NTP ロギング	無効
NTP 流通	ディセーブル

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。